xIlkogretim Online - Elementary Education Online,2021; Vol 20 (Issue 1): pp.2342-2348
http://ilkogretim-online.org
doi: 10.17051/ilkonline.2021.01.261

Smart City Development Using Efficient Cryptography For Image Processing

S. Pavithradevi, Department of ECE, College of Engineering, SRM Institute of Science and Technology, Kattankulathur, Kancheepuram-603203.
K. Vadivukkarasi, Department of ECE, College of Engineering, SRM Institute of Science and Technology, Kattankulathur, Kancheepuram-603203.
S. Krithiga, Department of ECE, College of Engineering, SRM Institute of Science and Technology, Kattankulathur, Kancheepuram-603203.
D.Vijayalakshmi, Department of ECE, College of Engineering, SRM Institute of Science and Technology, Kattankulathur, Kancheepuram-603203.

Abstract- In Internet of Things (IoT), there are many applications involved one among which is smart city. Smart city involves maintaining activities of the traffic system, CCTV surveillance camera which kept in many locations to monitor the abnormal activities, human movement detection, energy measurement etc. Among which, surveillance camera plays major role in security purpose. Basically, in smart city camera is kept on and it stores the entire situation happening around the environment which results in major challenge in the storage management and security level. To avoid this criteria, in this paper it conveys a scheme which enable CCTV surveillance system to store only when there is detection of any movement of human and occurring of any abnormal event in city. A new approach is performed in modifying the Advanced Encryption Standard method for smart city which is IoT based system. The main aim of this cryptography is to maintain the storage management efficiently and also it provides lesser execution time by providing less weight age in processing an image than other cryptography mechanism.

Keywords: cryptography, private key, color image, image processing, CCTV surveillance

I. INTRODUCTION

Internet of Things has enormous attraction from business, industry, transport, smart cities and academic sector. It monitors an environment and it gathers data from the environment using sensors to transmit and receive information collected with peer nodes to perform automated services and work [1]. Usually, Smart city have advantage in retrieving and storing the important data which is embedded with video footage of incident happened in particular location via unsecured network resulting to hacking of data [2]. This approach has a strategy over private key cryptosystem resulting in advancement in storage management [3]. In proposed system, secured transmission of data (i.e. recorded video, image) can be obtained using generated private key. In Rapid development of information technology [4], security has major role in sharing and retrieving of the data across the location especially Video recording from the surveillance system, has to be maintained for future reference [5]. To avoid recording of the camera during non-occurrence of any event, proposed scheme plays a vital role. Proposed scheme helps in secure transmission also it has major advantage over existing in accuracy, execution time and storage management. The major motivation is to reduce the storage of data in server, concealed way of storing them in IoT and sharing of data, (CCTV surveillance) within two parties without interruption of third one.

A simple approach is utilized which involves recording video or photos with CCTV Camera and it detects the motion of human based on which some algorithm is applied to share the data securely [6]. The main disadvantage is even there is no detection of human motion it get recorded. In Internet of Things, remote login access is limited, slow frame, different calculation and requires memory to consume huge data [7]. So, here it provide compact enough to save storage of large data sets, data Privacy and the fine grained access control. Furthermore, encrypted data can be reduced through file conversion from one format to other format.

II. RELATED WORKS

Public key cryptosystem is utilized in which the private key is for decryption to avoid hacking of data which is shared securely [8]. A model is approached in which a new protocol is used named UAKMP [User Authenticated Key Management Protocol] which is an offline sensing node registration. The security method includes authentication and key agreement. Medical data played a major role which includes gene, Electroencephalogram signal and Electronic medical data. Rivets, Shamir and Adleman (RSA) also named as asymmetric cryptographic method [9]. It involves new sensing node deployment [10]. Chaotic image encryption involves with two main steps; [11], one is pixel permutation and other is pixel diffusion named as symmetric encryption type [12]. Modified AES algorithm is used to approach cryptographic mechanism in IoT [13]. In heterogeneous encryption, KP-ABE is an algorithm used for implementing an access control and security mechanism. In this paper, they utilized three sections for IoT security: first section is combination of initialization and key generation, second section is encryption process and last section involves decryption [14].

III. SYSTEM ARCHITECTURE

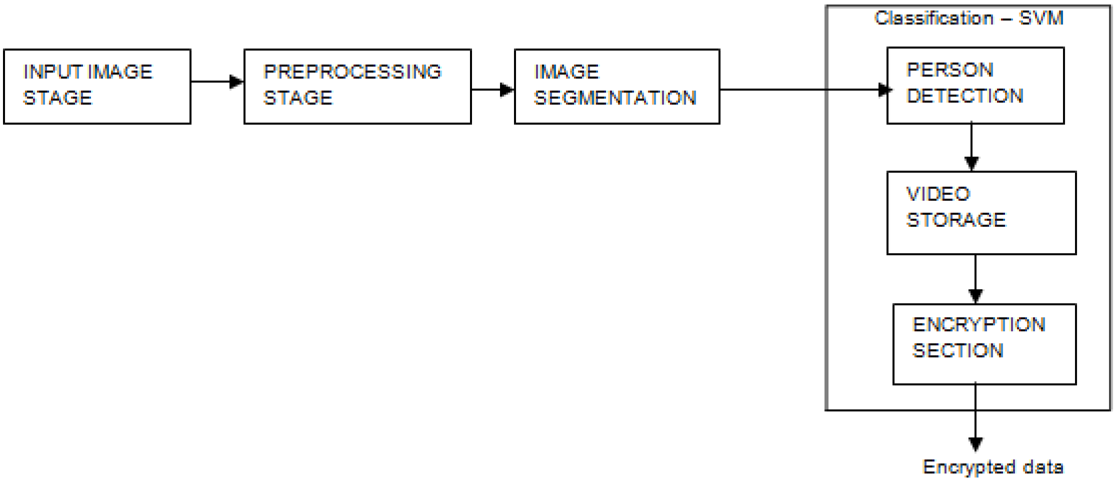


Figure 1. Flow of collecting an input image to converting the gathered image to other form

In Figure 1, input image stage is an initial stage (image acquisition) which is occurred in any vision system. Different processing methods is involved after the collection of an image, awful task may not be achievable when the captured image is not satisfactory [15]. After gathering information (video footage, image etc.) from CCTV Surveillance camera, it is processed for next stage (gray level) by preprocessing stage. Histogram equalization is performed here for preprocessing technique which is explained in equation (1).

$$\mathrm{S_k} = \sum_{\mathrm{j=0}}^{\mathrm{k}} \mathrm{P_r}\ \mathrm{r(j)} \quad \mathrm{for} \quad 0 \leq \mathrm{k} \leq \mathrm{L} - 1 \qquad (1)$$

The termP_r r(j) $= \frac{n_j}{n}$represents number of pixel with gray level r (j) to the total number of pixels.

In image processing, the frame is extracted from video to modify into grayscale. In image segmentation Region of Interest is performed which is occurred after segmenting into multiple frames from previous stage. By using known values, statics is applied to correlate the image. In classification, get the data i.e. video from the CCTV surveillance camera and apply moving object detection algorithm based on Support Vector Machine method. Extract the moving object and identify types of situation like night, evening time, heavily congested area and also bad weather condition such as fog and rain based on which apply different image processing techniques to compare the results with the already available algorithm and convert the video into text file to save the best one in a database.

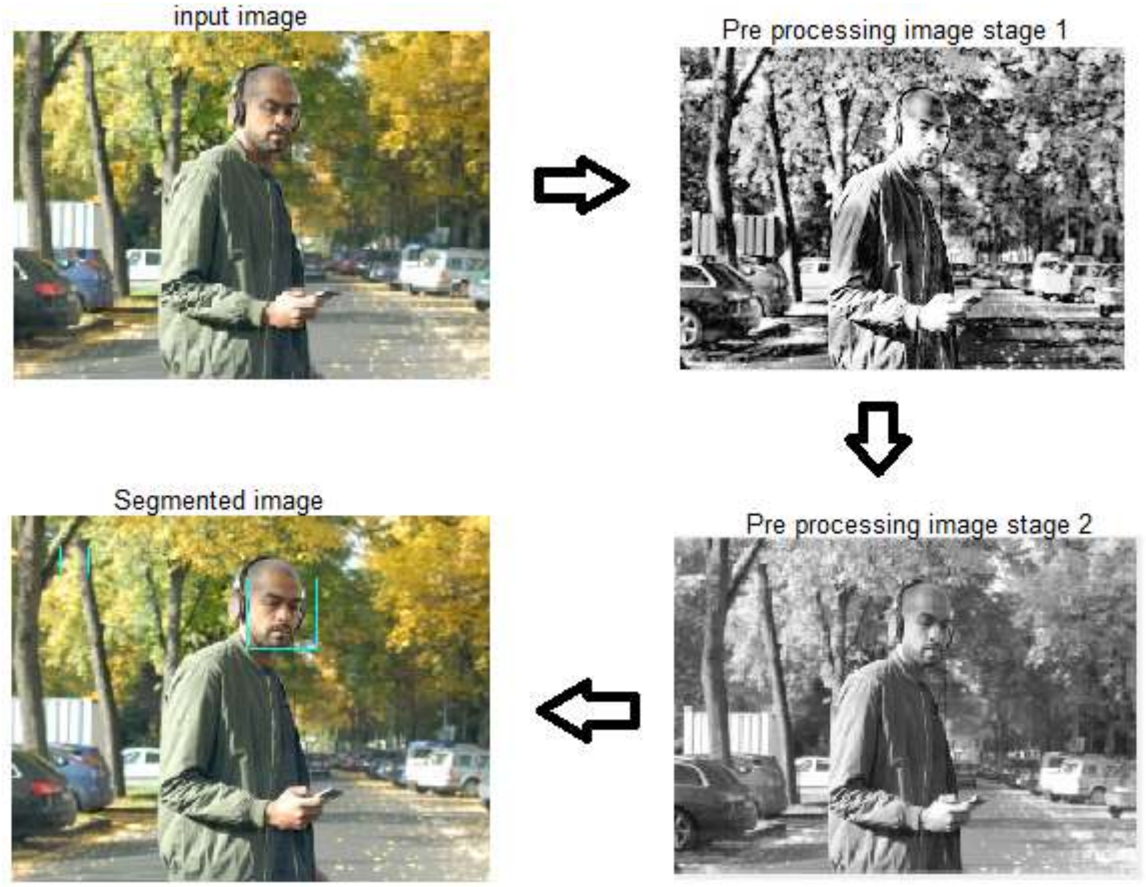


Figure 2. a. Processing of an image from collected raw data into segmentation which involves detection of human before entering encryption method.

Entire function has been done by SVM algorithm which is expressed as follow,

$$f(x_i) = \frac{1}{n}\left[\sum \max\big(0,1 - y_i(w.x_i - b)\big)\right] + \lambda|w|^2 \qquad (2)$$

In above equation (2), xi represent data point i, w is the decision hyper plane normal plane and yi is class of data point i.

IV. CRYPTOGRAPHIC MECHANISM

Basically in cryptography, key is maintained which is shared or secretly maintained by the parties to securely share and retrieve the data (video, image, etc.).Here, private key is used which can be used to retrieve the information by the party from other side. Figure 2.b show the flow of execution from data collection to encryption and retrieving data from the cloud for decryption.

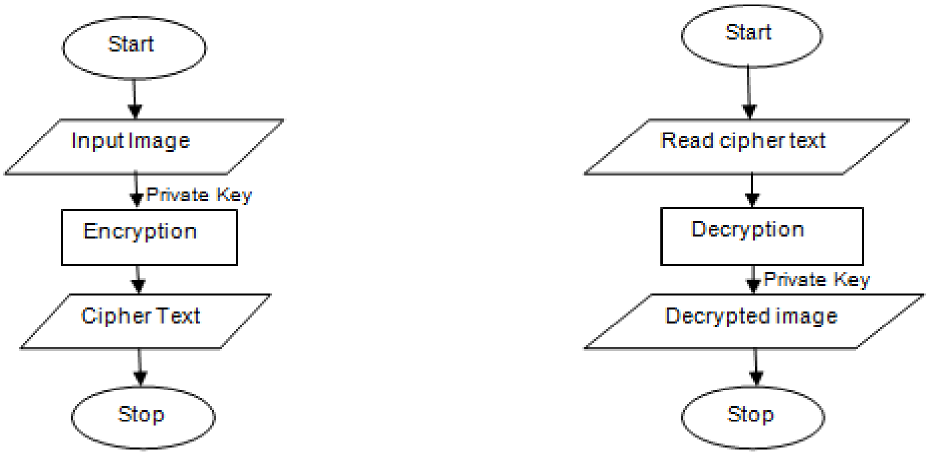


Figure 2.b Encryption and Decryption

Usually in AES, the encryption is performed by using plaintext XOR with the key generated and it tends to store the cipher text. In this approach, the less weight age is provided for plaintext then succeeded with encryption which provides less storage for cipher text than Advanced Encryption Standard. Figure 3 explains the generation of key later encrypting the collected image into unreadable format. In Image, pixel is the basic element which is get modified in usual encryption process alternatively in this paper, technique is approached which assign weight to the pixel value and it is initiated with encryption.

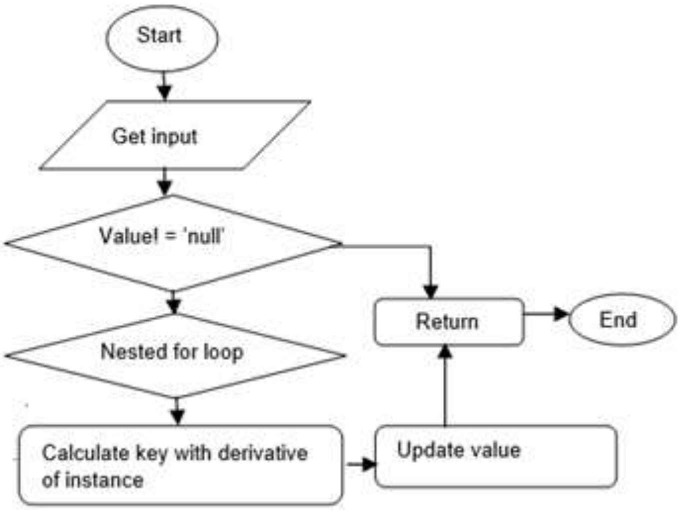


Figure 3. Flow of key generation

Derivative of instance is calculated in meanwhile process to eliminate the negative value for key generation (k). In below equation, x (i) and y (j) represent the pixel value of an image located in rows and column to provide with weight age value.

$$u = \sin x(i) * \cos y(j) \qquad (3)$$

$$v = \sin x(i) + \cos y(j) \qquad (4)$$

Equation (5) and (6) represented to avoid the repeat of same value to similar pixel which is in different location of same image resulting in key generation.

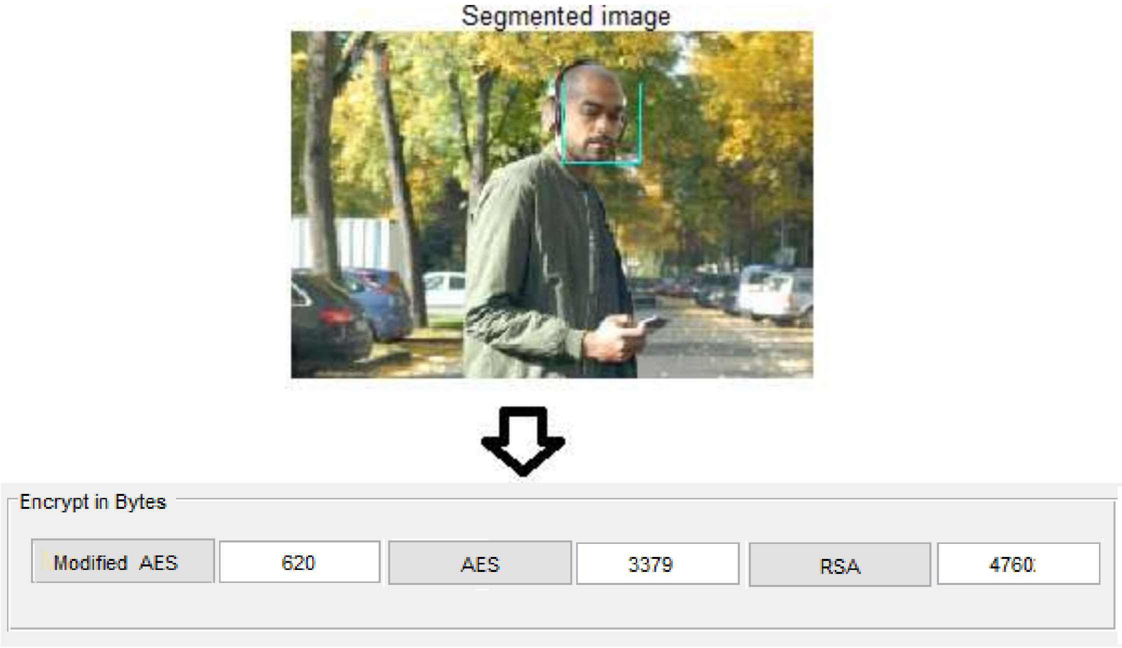
$$w = x(i) * \exp(x(i)^2 - y(j)^2) \qquad (5)$$

$$key(i, j, time) = ({}^{1}/_{dt} + {}^{u}/_{dx} + {}^{v}/_{dy} + {}^{w}/_{dz}) \qquad (6)$$

Result of above process is explained in figure 4 which shows maintaining the storage efficiently than other cryptographic mechanism. The generated key is stored in a file rather than calculating again. Since multi key is used it makes the mechanism difficult in predicting the key. The generated key is of 128 bit length used along with data for encryption which take nearly 10 rounds based on key length in AES. Encryption is performed for converting plain text (P) into cipher text (C) with key generated (k) by equation (7).

$$Cipher\ Text = PlainText\ stream \oplus key\ generated \qquad (7)$$

V. RESULT



Encrypt in Bytes

Modified AES 620 AES 3379 RSA 4760

Figure 4. Segmented image into Encrypted image in bytes

The segmented image is introduced to encryption here in figure 4 the size of cipher text is shown in bytes. Figure5.a explains that plain text differ from 30 KB to 300 KB and encrypted file size (cipher text) represented in x-axis and y-axis respectively. The improvement in proposed is clearly mentioned in figure 5.a that cipher text size is less than Advanced Encryption Standard and Rivets Shamir and Adleman method. Figure5.b shows that proposed scheme requires less execution time than other two cryptography method (RSA, AES) but time depends on the file size. For 30 KB file size, encryption time required is 2 ms for proposed scheme. Since, less weight age is assigned for pixel it makes mechanism as efficient in cipher text size and execution time than other model.

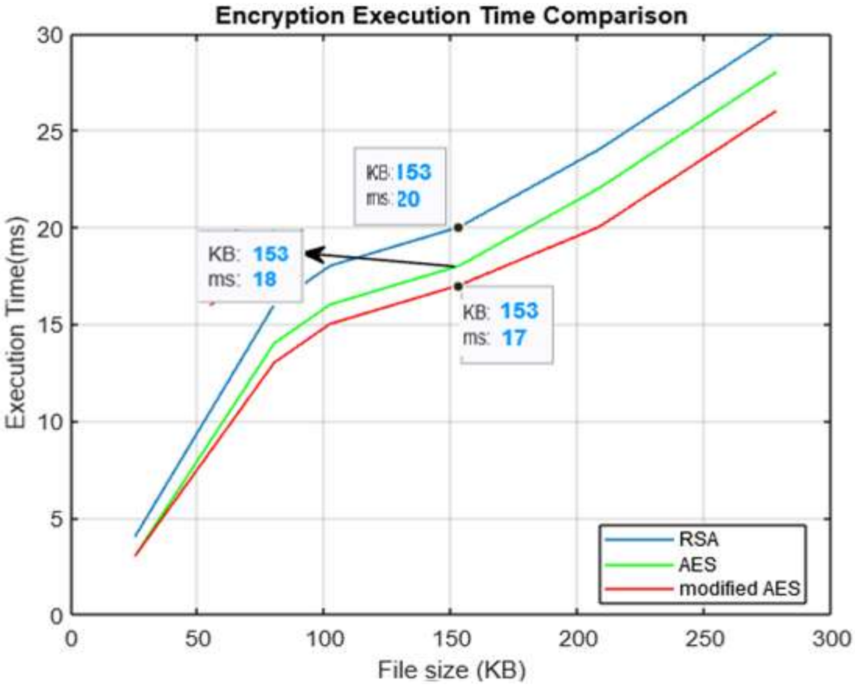


Figure 5.a. Comparing Encryption Execution Time for RSA, AES and modified AES

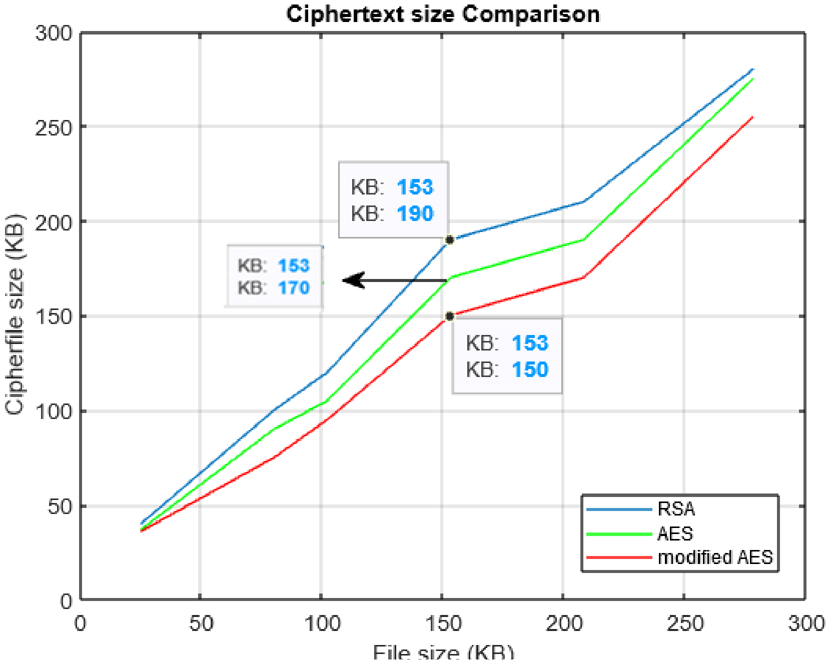


Figure 5. b. Comparing Cipher Text size with the plain Text files size for RSA, AES and modified AES

VI. CONCLUSION

The proposed scheme has more advantage over existing in calculation of key generation and execution time. The storage management is also performed effectively than other cryptography. Since private key is used management of key is done efficiently. Future research is based on the development of secure transmission in cryptography mechanism which has vital role in Internet of Things also to achieve decentralization in IoT for easier remote access.

References

1. Jan MA, Khan F, Alam M, Usman M (2019) A payload-based mutual authentication scheme for Internet of Things. Future General Computing System.
2. Edward YellakuorBaagyere, peter Awon-natemiAgbedemnab, En Qin , Mohammed Ibrahim Daabo, and Zhiguang Qin(2019),” A multi-layered data encryption and decryption scheme based on genetic algorithm and residual numbers”, in IEEE.
3. Babayiğit B, Büyükpatpat B (2019) Design and implementation of IoT-based irrigation system. IntConfComputSciEng (UBMK).
4. Maria Stoyanova, YannisNikoloudakis, SpyridonPanagiotakis, EvangelosPallis, and Evangelos K. Markakis (2019),”A survey on the Internet of Things (IoT) Forensics: challenges , approaches and open issues” in IEEE Communication survey .
5. SaadAlabdulsalam, Kevin Schaefer, TaharKechadi and Nhien-An Le-Khac,(2018)”internet of things forensics –challenges and a case study”, International Federation for Information Processing, springer .
6. Qiu J, Du L, Zhang D, Su S, Tian Z (2020) Nei-TTE: Intelligent Traffic Time Estimation Based on Fine-Grained Time Derivation of Road Segments for Smart City, IEEE
7. M. Wazid, A. K. Das, N. Kumar, M. Conti, and A. V. Vasilakos(2017), “A Novel authentication and Key Agreement Scheme for Implantable Medical Devices deployment,” IEEE Journal of Biomedical and Health Informatics.
8. Xiang Wu, Yongting Zhang, Aming Wang, Minyu Shi , Huanhuan Wang ,Lian Liu (2019) Medical big data privacy protection platform basedon Internet of things. Neural Computing and Applications, Springer.
9. Mohammad Wazid, Ashok Kumar Das, VangaOdelu, Neeraj Kumar, Mauro Conti, and Minho Jo(2017), Design of Secure User Authenticated Key Management Protocol for Generic IoT Networks, IEEE Internet of Things
10. RongjunGe, Guanyu Yang, Jiasong Wu ,Yang Chen Luo(2019), A Novel Chaos-Based Symmetric Image Encryption Using Bit-Pair Level Process, IEEE Access
11. Touati L, Challal Y (2016) Collaborative KP-ABE for cloud-based Internet of Things pplications. IEEE IntConfCommun (ICC).
12. Khader M, Alian M, Hraiz R, Almajali S (2017) Simplified AESalgorithm for ealthcare applications on Internet of Thing. IntConf Inform Technol (ICIT).
13. M. Wazid, A. K. Das, N. Kumar, and J. P. C. Rodrigues (2017), “Secure Three factorUser Authentication Scheme for Renewable Energy Based Smart Grid Environment,” IEEE Transactions on Industrial Informatics.
14. P. P. Bhangale, A. Gawad, J. Maurya, and R. S. Raje (2017),Image security using AES and RNS with reversible watermarking,'' International journal Innovation of Science Engineering and Technology.
15. G. C. Kessler. (2020). *An Overview of Cryptography*.Garykessler.net. Accessed: [Online]. Available: https://www.garykessler.net/library/crypto.html.